Attorney Docket No. 1793.1186

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Jong-ha LEE et al.

Application No.: Group Art Unit:

Filed: January 21, 2004 Examiner:

For: USER AUTHENTICATION METHOD AND APPARATUS

SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application:

Republic of Korea Patent Application No(s). 2003-4104

Filed: January 21, 2003

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date(s) as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: January 21, 2004 By: _____
Michael D. Stein
Registration No. 37,240

1201 New York Ave, N.W., Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

대한민국특허청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 10-2003-0004104
Application Number

출 원 년 월 일 : 2003년 01월 21일
Date of Application JAN 21, 2003

출 원 인 : 삼성전자주식회사
Applicant(s) SAMSUNG ELECTRONICS CO., LTD.

2003 년 02 월 07 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【참조번호】	0010
【제출일자】	2003.01.21
【국제특허분류】	G06F
【발명의 명칭】	사용자 인증 방법 및 장치
【발명의 영문명칭】	Method and Apparatus for user authentication
【출원인】	
【명칭】	삼성전자 주식회사
【출원인코드】	1-1998-104271-3
【대리인】	
【성명】	이영필
【대리인코드】	9-1998-000334-6
【포괄위임등록번호】	2003-003435-0
【대리인】	
【성명】	이해영
【대리인코드】	9-1999-000227-4
【포괄위임등록번호】	2003-003436-7
【발명자】	
【성명의 국문표기】	이종하
【성명의 영문표기】	LEE,Jong Ha
【주민등록번호】	740117-1691611
【우편번호】	445-974
【주소】	경기도 화성군 태안읍 병점리 우남드림밸리 1차아파트 104동 301호
【국적】	KR
【발명자】	
【성명의 국문표기】	황의현
【성명의 영문표기】	HWANG,Eui Hyeon
【주민등록번호】	720920-1067323
【우편번호】	420-751

【주소】	경기도 부천시 원미구 상1동 반달마을아파트 1804동 1705호
【국적】	KR
【심사청구】	청구
【취지】	특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사 를 청구합니다. 대리인 이영필 (인) 대리인 이해영 (인)
【수수료】	
【기본출원료】	20 면 29,000 원
【가산출원료】	20 면 20,000 원
【우선권주장료】	0 건 0 원
【심사청구료】	46 항 1,581,000 원
【합계】	1,630,000 원
【첨부서류】	1. 요약서·명세서(도면)_1통

【요약서】

【요약】

사용자 인증 방법이 개시된다. 본 발명에 따른 그림 암호에 의한 사용자 인증 방법은, 그림 암호가 입력되었는가를 판단하는 단계; 입력된 그림 암호의 정합 정도에 따라 사용자 인증 여부를 결정하는 단계; 인증되지 않은 경우에는 그림 암호 입력 히스토리를 저장하는 단계; 그림 암호 입력 히스토리를 이용하여 침입 여부를 결정하는 단계; 및 침입이라고 결정된 경우, 인증 마진을 감소시키는 단계를 포함한다. 또한 본 발명에 따른 그림 암호와, 생체 인식 정보에 의한 사용자 인증 방법은, (a) 상기 그림 암호가 입력되었는가를 판단하는 단계; (b) 상기 그림 암호가 입력된 경우에, 상기 입력된 그림 암호의 정합 정도에 따라 생체 인식의 문턱값을 가변하여 설정하는 단계; (c) 외부로부터 입력된 사용자의 생체 인식 정보와 등록된 생체 인식 정보를 비교하여 사용자가 인증되었는가를 판단하고, 사용자가 인증되지 않은 경우에는 상기 (a) 단계로 진행하는 단계를 포함한다. 따라서, 키 조작부가 없는 PDA 등에서의 그림 암호에 의한 사용자 인증에 있어서, 편의성, 신뢰성 및 보안성을 확보할 수 있다. 또한 그림 암호에 의한 사용자 인증 결과에 따라 생체 인식을 위한 문턱값을 가변함으로써, 생체 인식기의 불완전한 인증 성능을 개선하여, FAR(False Acceptance Rate)과 FRR(False Rejection Rate)을 동시에 낮출 수 있다.

【대표도】

도 1

【명세서】

【발명의 명칭】

사용자 인증 방법 및 장치{Method and Apparatus for user authentication}

【도면의 간단한 설명】

도 1은 본 발명에 의한 그림 암호에 의한 사용자 인증방법의 바람직한 일 실시예를 설명하기 위한 플로우차트이다.

도 2는 본 발명에 의한 그림 암호와 생체 인식에 의하여 사용자를 인증하는 방법의 바람직한 일 실시예를 설명하기 위한 플로우차트이다.

도 3은 본 발명에 의한 그림 암호와 생체 인식에 의하여 사용자를 인증하는 방법의 바람직한 다른 실시예를 설명하기 위한 플로우차트이다.

도 4는 본 발명에 의한 그림 암호와 생체 인식에 의하여 사용자를 인증하는 방법의 바람직한 또 다른 실시예를 설명하기 위한 플로우차트이다.

도 5는 본 발명에 의한 사용자 인증 방법을 수행하는 사용자 인증 장치의 바람직한 일 실시예의 구성을 설명하기 위한 블록도이다.

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<6> 본 발명은 사용자 인증에 관한 것으로서, 특히 그림 암호에 의한 사용자 인증 및 생체 인식에 의한 사용자 인증에 관한 것이다.

<7> 암호와 관련된 종래 사용자 인증 기술로는 다음과 같은 것들이 있다.

<8> 국내특허출원 제1999-56333호 "비밀번호 시스템"은 각종 보안 경보장치나, 금고나, 출입문이나 PC나 은행 ATM기 등의 키패드 수단으로 입력하는 비밀번호 시스템에 있어서, 실제 비밀번호를 구성하는 숫자나 문자나 부호를 진수로 하고, 비밀번호로서 뜻이 없는 숫자나 문자나 부호를 허수로 하여 허수와 진수를 조합하여 비밀번호를 구성하고 허수에 특정한 비밀명령 신호를 부여하여 비밀번호에 고유의 비밀번호로서의 기능과 비밀 명령어 삽입기능이 가능한 비밀번호 시스템을 개시하고 있다.

<9> 국내특허출원 제1999-59247호 "이동 무선 전화기의 잠금 기능 설정/해제 방법"은 연상 문구 입력 기능 선택을 감지하고 연상 문구를 입력하여 메모리에 저장하는 제1과정과, 잠금 상태에서 파워 오프되었다가 다시 파워 온되었음을 감지하면 비밀번호 입력 요구 화면을 표시한 다음, 입력되는 비밀번호와 미리 저장된 비밀번호를 비교하여 일치 여부를 판단하되 정해진 횟수 이상 반복해도 일치되지 않으면 메모리로부터 연상 문구를 읽어 화면에 표시하는 제2과정으로 이루어져 있다.

<10> 국내특허출원 제2000-8580호 "인터넷상의 비밀번호 입력 시스템 및 그 입력 방법"은 화면상에 표시된 그림의 특정 영역을 클릭하여 비밀번호를 입력하는 인터넷상의 비밀번호 입력 시스템과 비밀번호 입력 방법이 개시되어 있다.

<11> 미국특허 US5,559,961 "Graphical password" 는 정해진 그림상의 특정 영역을 터치(touch)함으로써 암호를 입력하는 수단이 개시되어 있다. 또한, 그림 상에서 탭 영역(tap region)을 설정하여 키 패드(key pad)처럼 사용할 수 있다.

<12> 한편, 암호와 생체 인식기를 결합한 형태의 종래 사용자 인증 기술로는 다음과 같은 것들이 있다.

<13> 국내특허출원 제2000-19152호 "휴대용 보안 인증 장치 및 시스템 그리고 그의 동작 방법"은 지문, 음성등의 생체 인증과 패스워드 입력의 순차적 결합에 의한 인증 방법을 개시하고 있다.

<14> 국내특허출원 제2000-3099호 "지문 인증과 비밀번호 인증 겸용 방식을 채용한 도어록/언록 시스템 및 그 제어 방법"은 지문등록이 불가능한 사용자의 사용을 가능하게 함과 동시에 지문등록이 이루어지지 않은 방문객도 비밀번호를 사용하여 사용자 인증을 받을 수 있는 지문인증과 비밀번호 인증 겸용방식을 채용한 도어 록/언록 시스템 및 그 제어방법을 개시하고 있다.

<15> 국내특허출원 제2000-60312호 "지문 인식 및 얼굴 인식을 이용한 출입 통제 시스템 및 그 방법"은 지문 인식과 얼굴 인식을 통한 사용자 인증, 비밀번호인증과 지문 인식과 얼굴 인식을 통한 사용자 인증, 및 인증되지 않은 출입자의 지문 및 얼굴을 저장하여 보안성을 향상시키는 출입 통제 시스템 및 그 방법을 개시하고 있다.

<16> 그 밖에 국내특허출원 제2001-15559호 "지문인식을 이용한 도어개폐시스템", 국내특허출원 제1999-26726호 "음성인식을 통한 휴대폰의 비밀번호 인식방법" 등 다수가 있다.

<17> 전술한 종래의 사용자 인증 기술들은 암호와 생체인식, 또는 보안열쇠와 생체인식을 단순히 결합하여 복수의 인증 절차를 거치게 하는 형태이다.

<18> 얼굴, 지문, 홍체 등의 인증키에 의한 생체인식기는 사용 환경, 사용자의 사용습관, 시간에 따른 인증키의 변화 등으로 인하여 인증키 자체가 생체 인식기에 다르

게 입력되어 인식 성능이 저하된다. 또한 생체 인식기의 문턱값 설정에 따라 등록된 사람이 인증되지 못하거나, 등록되지 않은 사람이 인증되는 오류가 발생하게 된다.

<19> 근래에 들어 개인용 휴대 단말기(PDA, Personal Digital Assistant)와 같이 그래픽 사용자 인터페이스를 통하여 사용자의 지시를 입력하는 장치의 사용이 증가하고 있다. 따라서, PDA 등에서의 그림 암호에 의한 사용자 인증에 있어서, 얼마나 인증의 편의성, 신뢰성 및 보안성을 확보하느냐 하는 것이 문제이다.

<20> 또한 그림 암호에 의한 사용자 인증과 생체 인식에 의한 사용자 인증을 결합함에 있어서, 그림 암호에 의한 인증과정이 이어지는 생체 인식에 의한 인증과정에 유기적으로 기여하도록 함으로써, 생체 인식기의 불완전한 인증 성능을 개선하도록 한다.

【발명이 이루고자 하는 기술적 과제】

<21> 본 발명이 이루고자 하는 기술적 과제는, 그림 암호(Graphical Password)에 의한 사용자 인증 방법을 제공하는 데 있다.

<22> 본 발명이 이루고자 하는 다른 기술적 과제는, 그림 암호 및 생체 인식이 유기적으로 결합된 형태의 사용자 인증 방법을 제공하는데 있다.

<23> 본 발명이 이루고자 하는 또 다른 기술적 과제는, 상기 그림 암호에 의한 사용자 인증 방법을 수행하는 사용자 인증 장치를 제공하는데 있다.

<24> 본 발명에 이루고자 하는 또 다른 기술적 과제는, 상기 그림 암호 및 생체 인식에 의한 사용자 인증 방법을 수행하는 사용자 인증 장치를 제공하는데 있다.

【발명의 구성 및 작용】

<25> 상기한 본 발명에 의한 기술적 과제를 이루기 위하여, 단말기 화면상에서 그래픽 사용자 인터페이스를 통해 입력된 그림 암호에 의해 사용자를 인증하는 본 발명에 의한 사용자 인증 방법은, 상기 그림 암호가 입력되었는가를 판단하는 단계; 상기 그림 암호가 입력된 경우에, 상기 입력된 그림 암호의 위치와 등록된 그림 암호의 기준 위치와의 정합 정도가 기준위치에 대한 인증 마진 이내인지 아닌지에 따라 사용자 인증 여부를 결정하는 단계; 인증되지 않은 경우에는 그림 암호 입력 히스토리를 저장하는 단계; 상기 그림 암호 입력 히스토리를 이용하여 침입 여부를 결정하는 단계; 및 침입이라고 결정된 경우, 상기 기준위치에 대한 입력 위치의 인증 마진을 감소시키는 단계를 포함하는 것이 바람직하다.

<26> 본 발명에 의한 다른 기술적 과제를 이루기 위하여, 단말기 화면상에서 그래픽 사용자 인터페이스를 통해 입력된 그림 암호와, 생체 인식 정보에 의하여 사용자를 인증하는 본 발명에 의한 사용자 인증 방법은, (a) 상기 그림 암호가 입력되었는가를 판단하는 단계; (b) 상기 그림 암호가 입력된 경우에, 상기 입력된 그림 암호와 등록된 그림 암호의 정합 정도에 따라 생체 인식의 문턱값을 가변하여 설정하는 단계; (c) 외부로부터 입력된 사용자의 생체 인식 정보와 등록된 생체 인식 정보를 비교하여 사용자가 인증되었는가를 판단하고, 사용자가 인증되지 않은 경우에는 상기 (a) 단계로 진행하는 단계를 포함하는 것이 바람직하다.

<27> 본 발명에 의한 또 다른 기술적 과제를 이루기 위하여, 단말기 화면상에서 그래픽 사용자 인터페이스를 통해 입력된 그림 암호에 의해 사용자를 인증하는 본 발명에 의한 사용자 인증 장치는, 상기 그림 암호가 입력되었는가를 판단하는 그림 암호 입력부; 상

기 그림 암호가 입력된 경우에, 상기 입력된 그림 암호의 위치와 등록된 그림 암호의 기준 위치와의 정합 정도가 기준위치에 대한 인증 마진 이내인지 아닌지에 따라 사용자 인증 여부를 결정하는 제어부; 상기 등록된 그림 암호를 저장하고 있고, 인증되지 않은 경우에는 그림 암호 입력 히스토리를 저장하는 저장부; 상기 그림 암호 입력 히스토리를 이용하여 침입 여부를 결정하는 그림 암호 입력 히스토리 분석부를 포함하는 것이 바람직하며, 침입이라고 결정된 경우에 상기 제어부는, 상기 기준위치에 대한 입력 위치의 인증 마진을 감소시키는 것을 특징으로 한다.

<28> 본 발명에 의한 또 다른 기술적 과제를 이루기 위하여, 단말기 화면상에서 그래픽 사용자 인터페이스를 통해 입력된 그림 암호와, 생체 인식 정보에 의하여 사용자를 인증하는 본 발명에 의한 사용자 인증 장치는, 상기 그림 암호가 입력되었는가를 판단하는 그림 암호 입력부; 등록된 그림 암호 및 등록된 생체 인식 정보를 저장하고 있는 저장부; 상기 그림 암호가 입력된 경우에, 상기 입력된 그림 암호와 등록된 그림 암호의 정합 정도에 따라 생체 인식의 문턱값을 가변하여 설정하는 제어부; 외부로부터 입력된 사용자의 생체 인식 정보와 등록된 생체 인식 정보를 비교하여 사용자가 인증되었는가를 결정하는 생체 인식부를 포함하는 것이 바람직하다.

<29> 이하, 본 발명에 의한 사용자 인증 방법 및 이를 수행하는 장치의 구성과 동작을 첨부한 도면들을 참조하여 다음과 같이 설명한다.

<30> 본 발명은 개인용 휴대 단말기(PDA, Personal Digital Assistant) 등의 화면상에서 그래픽 사용자 인터페이스를 통해 입력된 그림 암호 또는/및 생체 인식에 의한 사용자 인증 방법에 관한 것이다.

<31> 도 1은 본 발명에 의한 그림 암호에 의한 사용자 인증방법의 바람직한 일 실시예를 설명하기 위한 플로우차트로서, 그림 암호를 입력 단계(S100 단계), 사용자 인증 결정 단계(S102 단계), 그림 암호 입력 히스토리 저장 단계(S104 단계), 히스토리를 이용한 침입여부 결정 단계(S106 단계) 및 침입자에 대한 인증 마진 감소 단계(S108 단계)를 포함한다.

<32> 본 발명의 첫 번째 사상은 단말기 화면상에서 그래픽 사용자 인터페이스를 통해 입력된 그림 암호에 의해 사용자를 인증하는 방법 및 장치에 관한 것이다.

<33> 먼저 S100 단계에서는, 그림 암호가 입력되었는가를 계속적으로 판단한다.

<34> S102 단계에서는, 그림 암호가 입력된 경우에, 상기 입력된 그림 암호의 위치와 등록된 그림 암호의 기준 위치와의 정합 정도가 기준위치에 대한 인증 마진 이내인지 아닌지에 따라 사용자 인증 여부를 결정한다. 또한, 사용자 인증 여부를 결정하는 S102 단계는, 그림 암호가 둘 이상의 입력의 조합으로 이루어지는 경우에, 그림 암호 입력 순서의 정합 정도에 따라 사용자 인증 여부를 결정하는 단계를 포함할 수도 있다.

<35> 여기서, 등록된 기준 위치는 소정 영역이 될 수 있다. 이 때, 소정 영역내에 그림 암호가 입력되면 그림 암호와 일치하는 것으로 판단한다.

<36> S104 단계에서는, 인증되지 않은 경우에는 그림 암호 입력 히스토리를 저장한다.

<37> S106 단계에서는, 그림 암호 입력 히스토리를 이용하여 침입 여부를 결정한다. 예컨대, 잘못된 순서로 암호가 입력된 회수 또는 인증 마진 밖에 암호가 입력된 회수가 n 회 이상이면 침임으로 결정한다. 그림 암호가 등록된 기준 위치로부터 소정 차단 거리 밖에 입력된 경우에는, 암호 입력 회수에 관계 없이 침입이라고 결정할 수도 있다. 기준

위치가 소정 영역으로 설정된 경우에는, 영역의 경계로부터 소정 차단 거리 밖에 그림 암호가 입력된 경우에 침입이라고 결정하게 된다.

<38> S108 단계에서는, 침입이라고 결정된 경우, 기준위치에 대한 입력 위치의 인증 마진을 감소시킨다.

<39> 본 발명에 의한 사용자 인증 방법은, 침입이라고 결정되어 인증 마진이 감소된 후에, 그림 암호의 입력 히스토리를 분석한 결과 침입 결정을 해제할 수 있다고 판단되는 경우에는, 감소된 인증 마진을 회복시키는 단계를 더 포함할 수도 있다. 예컨대, S102 단계의 판단 결과 인증되지는 않았지만, 인증 마진의 경계로부터 소정 거리 이내의 위치에 그림 암호가 연속적으로 m회 이상 입력되면, 침입 결정을 해제하여 인증 마진을 회복시키도록 구현할 수 있다.

<40> 또한, 사용자로 하여금 그림 암호의 입력을 용이하게 하기 위하여, 배경 그림을 표시하는 단계를 더 포함할 수도 있다.

<41> 도 2는 본 발명에 의한 그림 암호와 생체 인식 정보에 의하여 사용자를 인증하는 방법의 바람직한 일 실시예를 설명하기 위한 플로우차트로서, 그림 암호 입력 단계(S200 단계), 그림 암호의 정합 정도에 따라 생체 인식의 문턱값을 가변하는 단계(S202 단계), 생체 인식에 의하여 사용자 인증 여부를 결정하는 단계(S204 단계)를 포함한다.

<42> 도 1에 도시된 실시예가 그림 암호에 의한 사용자 인증 방법의 일 실시예인데 비하여, 도 2에 도시된 실시예는 단말기 화면상에서 그래픽 사용자 인터페이스를 통해 입력된 그림 암호와 생체 인식이 결합한 형태의 사용자를 인증하는 방법의 일 실시예이다.

<43> S200 단계에서는, 그림 암호가 입력되었는가를 계속적으로 판단한다.

<44> S202 단계에서는, 그림 암호가 입력된 경우에, 입력된 그림 암호와 등록된 그림 암호의 정합 정도에 따라 생체 인식의 문턱값을 가변하여 설정한다. 여기서, 정합 정도는, 그림 암호의 입력 위치가 기준 위치로부터 얼마나 멀리 떨어졌는가에 따라 결정된다. 기준 위치는 소정 영역으로 설정될 수도 있으며, 이 때 소정 영역내에 그림 암호가 입력되면 그림 암호와 일치하는 것으로 판단한다. 또한, 둘 이상의 그림 암호가 설정된 경우에는 암호의 입력 순서에 따라서도 정합 정도가 결정될 수 있다.

<45> S202 단계는, 그림 암호는 항상 통과하되 그림 암호의 정합 정도에 따라 생체 인식의 문턱값만을 가변하도록 구현될 수 있다. 그림 암호의 정합 정도가 높을수록 FRR(False Rejection Rate, 주인이 거부될 확률)을 낮추는 방향으로 문턱값을 조정한다. 반대로 그림 암호의 정합 정도가 낮을수록 FAR(False Acceptance Rate, 타인이 침입할 확률)을 낮추는 방향으로 문턱값을 조정한다.

<46> 그림암호의 정합 정도에 따라 문턱값을 가변하는 구체적인 예를 다음과 같이 설명한다.

<47> 그림 암호 입력 위치(x)의 정합 정도에 따라 문턱값을 가변하는 문턱값 결정함수 t(x)의 예는 다음 수학식 1과 같다.

<48> 【수학식 1】 $$t(x) = t_0 + c|x - x_0|^n$$

<49> 여기서 x_0 는 등록된 기준 위치이며, $|x - x_0|$는 정합 정도이고, t_0 는 기준 문턱값이며, c는 소정 가중치이다. $t_0 = -0.72$, $n=2$, $c=7.5\times10^{-5}$ 인 경우에, 문턱값의 가변 범위 및 대응되는 FAR(%) 과 FRR(%) 의 설정 예는 표1과 같다.

<50> 【표 1】

문턱값	FAR(%)	FRR(%)
...	...	...
-0.68	1.028	7.361
-0.69	1.119	6.667
-0.70	1.234	6.389
-0.71	1.341	6.389
-0.72	1.488	6.250
-0.73	1.599	6.111
-0.74	1.750	6.111
-0.75	1.913	5.972
...	...	...

<51> 또한 S202 단계는, 그림 암호 입력에 따라 사용자 인증 여부를 일차적으로 결정하고, 그림 암호 입력에 의하여 사용자가 인증된 경우에만, 생체 인식에 의한 사용자 인증 과정을 거치도록 구현될 수 있다. 그림 암호 입력에 의하여 사용자가 인증된 경우에, 그림 암호의 정합 정도에 따라 문턱값을 가변하도록 구현할 수 있다. 그림 암호의 정합 정도가 높을수록 FRR을 낮추는 방향으로 문턱값을 조정한다. 반대로 그림 암호의 정합 정도가 낮을수록 FAR을 낮추는 방향으로 문턱값을 조정한다.

<52> S204 단계에서는, 외부로부터 입력된 사용자의 생체 인식 정보와 등록된 생체 인식 정보를 비교하여 사용자가 인증되었는가를 판단하고, 사용자가 인증되지 않은 경우에는 S200 단계로 진행한다.

<53> 도 3은 본 발명에 의한 그림 암호와 생체 인식에 의하여 사용자를 인증하는 방법의 바람직한 다른 실시예를 설명하기 위한 플로우차트로서, 그림 암호에 의해 사용자가 인증된 경우에만 생체 인식에 의한 사용자 인증을 거치도록 하는 단계들(S300 ~ S306 단계)을 포함한다.

<54> 먼저, 그림 암호가 입력된 경우에(S300 단계), 입력된 그림 암호의 위치와 등록된 그림 암호의 기준 위치와의 정합 정도가 기준위치에 대한 인증 마진 이내인지 아닌지에 따라 사용자 인증 여부를 결정한다(S302 단계). 여기서, S302 단계는, 그림 암호가 2 이상의 입력의 조합으로 이루어지는 경우에, 그림 암호 입력 순서의 정합 정도에 따라 사용자 인증 여부를 결정하는 단계를 포함할 수도 있다. 여기서, 등록된 기준 위치는 소정 영역이 될 수 있다. 이 때, 소정 영역내에 그림 암호가 입력되면 그림 암호와 일치하는 것으로 판단한다.

<55> S308 ~ S312 단계는 그림 암호에 의해 사용자가 인증되지 않은 경우에 선택적으로 더 포함되는 단계들이다.

<56> 만일 그림 암호에 의해 인증되지 않은 경우에는, 그림 암호 입력 히스토리를 저장한다(S308 단계). S308 단계 후에, 그림 암호 입력 히스토리를 이용하여 침입 여부를 결정한다(S310 단계). 예컨대, 잘못된 순서로 암호가 입력된 회수 또는 인증 마진 밖에 암호가 입력된 회수가 n회 이상이면 침임으로 결정한다. 그림 암호가 등록된 기준 위치로부터 소정 차단 거리 밖에 입력된 경우에는, 암호 입력 회수에 관계 없이 침입이라고 결정할 수도 있다. 기준 위치가 소정 영역으로 설정된 경우에는, 영역의 경계로부터 소정 차단 거리 밖에 그림 암호가 입력된 경우에 침입이라고 결정하게 된다. 만일 침입이라고 결정된 경우, 기준위치에 대한 입력 위치의 인증 마진을 감소시킨다(S312 단계).

<57> 본 발명에 의한 사용자 인증 방법은, 침입이라고 결정되어 인증 마진이 감소된 후에, 그림 암호의 입력 히스토리를 분석한 결과 침입 결정을 해제할 수 있다고 판단되는 경우에는, 감소된 인증 마진을 회복시키는 단계를 더 포함할 수도 있다. 예컨대, 소정 인증 마진 이내의 위치에 그림 암호가 연속적으로 m회 이상 입력되면, 침입 결정을 해제

하여 인증 마진을 회복시키도록 한다. 또한, 사용자로 하여금 그림 암호의 입력을 용이하게 하기 위하여, 배경 그림을 표시하는 단계를 더 포함할 수도 있다.

<58> 도 4는 본 발명에 의한 그림 암호와 생체 인식에 의한 사용자 인증 방법의 바람직한 또 다른 실시예를 설명하기 위한 플로우차트로서, 그림 암호의 입력 히스토리에 따라 침입여부가 결정되고 생체 인식 단계의 문턱값이 재설정되는 단계들(S400 ~ S416 단계)로 이루어진다. S400 단계 및 S402 단계는 전술한 도 2의 S200 단계 및 S202 단계와 동일하다.

<59> S402 단계 후에, 그림 암호 입력 히스토리를 저장한다(S404 단계).

<60> S404 단계 후에, 생체 인식에 의해 사용자가 인증되었는가를 판단한다(S406 단계).

<61> 만일 사용자가 인증된 경우에는 사용자 인증 방법을 종료한다. 그러나 만일 사용자가 인증되지 않은 경우에는 그림 암호 입력 히스토리를 이용하여 침입여부를 결정하여, 침입이 아니라고 결정되면 S400 단계로 진행한다(S412 단계). 여기서, S400 단계로 진행하기 전에 그림 암호 입력 히스토리를 이용하여 문턱값의 가변 범위를 변경하는 단계(S416 단계)를 선택적으로 더 포함할 수 있다. 예컨대 S416 단계는, 잘못된 그림 암호의 입력이 n회 이상인 경우에 보안 수준을 높이도록 상기 문턱값의 가변 범위를 변경하도록 구현될 수 있다. S400 단계에서, 생체 인식을 위한 문턱값의 가변 범위는 그림 암호의 정합 정도에 따라 소정 범위를 갖고 가변된다. S416 단계는 이 가변 범위를 변경하는 것이다. S416 단계는, 전술한 수학식 1에 의한 문턱값 가변 함수를 참조하면, 기준 문턱값 t_0 의 변경이나, 가중치 c 와 n의 변경에 의하여 문턱치의 가변 범위를 변경할 수 있다. 또한 S416 단계는, 수학식 1과는 다른 문턱값 결정함수로서 보안 수준을 높일 수도 있다.

<62> 또한 S416 단계는, 보안 수준을 높이도록 문턱값의 가변 범위를 변경한 후에, 올바른 그림 암호의 입력이 m회 이상이라고 판단된 경우, 문턱값의 가변 범위를 환원하는 단계를 더 포함할 수도 있다.

<63> S412 단계의 판단 결과 침입이라고 결정된 경우, 입력된 침입자의 생체 인식 정보를 저장하는 S414 단계를 더 포함할 수 있다. 이 때, S406 단계는 생체 인식 정보 입력값과 S414 단계에서 저장된 침입자의 생체 인식 정보를 비교하여 인증하는 단계를 포함할 수 있다.

<64> 한편, S406 단계에서 생체 인식에 의해 사용자가 인증된 경우에, 인증키를 추가/갱신하는 단계들(S408, S410 단계)를 더 포함할 수 있다. 즉 생체 인식의 인증키를 갱신할 것인가를 판단하여(S408 단계), 갱신할 것이라고 판단되면, 인증키를 추가 갱신한다(S410 단계). S408 단계는, 입력된 그림 암호가 등록된 그림 암호와 일치하고, 생체 인식에 의해 사용자가 인증된 경우에만 인증키를 추가/갱신하도록 결정할 수 있다. 또한 S408 단계는, 생체 인식에 의해 사용자가 인증된 경우, 입력된 생체 인식 정보와 등록된 생체 인식 정보의 정합 정도가 소정 문턱값 이상인 경우에만 인증키를 추가/갱신하도록 결정할 수도 있다.

<65> 도 5는 본 발명에 의한 사용자 인증 방법을 수행하는 사용자 인증 장치의 바람직한 일 실시예의 구성을 설명하기 위한 블록도로서, 그림 암호 입력부(10), 제어부(20), 저장부(30), 생체 인식부(40), 그림 암호 입력 히스토리 분석부(50) 및 표시부(60)를 포함한다. 도 5에 포함된 각 구성요소의 동작을 도 4에 도시된 사용자 인증 방법의 실시예와 대비하여 다음과 같이 설명한다.

<66> 그림 암호 입력부(10)는 도 4에 도시된 S400 단계를 수행하기 위하여, 휴대용 단말기 등의 화면상에 마련되어 그림 암호를 입력하는 수단이다.

<67> 표시부(60)는 휴대용 단말기 등의 디스플레이 화면에 해당하며, 그래픽 사용자 인터페이스를 구현하며, 배경 그림을 표시한다.

<68> 제어부(20)는 도 4에 도시된 S402 단계를 수행하기 위하여, 그림 암호의 정합정도에 따라 생체 인식을 위한 문턱값을 가변하여 설정한다. 또한 제어부(20)는 도 4에 도시된 S416 단계를 수행하기 위하여 그림 암호 입력 히스토리 분석부(50)의 분석 결과에 따라 문턱값의 가변 범위를 변경한다. 제어부(20)는 S408 단계를 수행하기 위하여 생체 인식 인증키를 갱신할 것인가를 부합하는가를 결정한다. 제어부(20)는, S412 단계를 수행하기 위하여, 그림 암호 입력 히스토리 분석부(50)의 분석 결과에 따라 침입 여부를 결정한다.

<69> 저장부(30)는 등록된 그림 암호 및 등록된 생체 인식을 위한 인증키를 저장한다. 인증키는 지문, 홍체, 얼굴 등이 될 수 있다. 저장부(30)는, S414 단계를 수행하기 위하여, 제어부(20)의 지시에 따라 생체 인식부(40)로 입력된 침입자의 생체 인식 정보를 저장한다. 또한 저장부(30), S410 단계를 수행하기 위하여, 제어부(20)의 지시에 따라 인증키를 추가/갱신하여 저장한다.

<70> 그림 암호 입력 히스토리 분석부(50)는, S406 단계 및 S412 단계를 수행하기 위하여, 그림 암호 입력 히스토리를 저장하고 이를 분석한다.

<71> 생체 인식부(40)는, S406 단계를 수행하기 위하여, 외부로부터 사용자의 생체 인식 정보를 획득하고, 획득된 생체 인식 정보와 저장부(30)에 등록된 생체 인식 정보를 비

교하여 정합 정도를 결정하고, 정합 정도가 문턱값 이상인 경우에 사용자를 인증한다. 또한 생체 인식부(40)는, 획득된 생체 인식 정보와 저장부(30)에 저장된 침입자의 생체 인식 정보를 비교하여, 사용자 인증 여부를 결정한다.

<72> 이하에서는, 도 5에 도시된 본 발명의 바람직한 일 실시예에 의한 사용자 인증 장치의 블록도를 참조하여, 도 1 내지 도 4에 도시된 사용자 인증 방법을 수행하는 사용자 인증장치의 구성 및 동작을 설명한다.

<73> 도 1에 도시된 사용자 인증 방법을 수행하는, 그림 암호에 의한 사용자 인증 장치는, 단말기 화면상에서 그래픽 사용자 인터페이스를 통해 입력된 그림 암호에 의해 사용자를 인증하기 위하여, 도 5의 구성요소 중에서 그림 암호 입력부(10), 제어부(20), 저장부(30), 그림 암호 입력 히스토리 분석부(50)를 포함한다.

<74> 도 1에 도시된 S100 단계를 수행하기 위하여, 그림 암호 입력부(10)는 그림 암호가 입력되었는가를 판단한다.

<75> S102 단계를 수행하기 위하여 제어부(20)는, 그림 암호가 입력된 경우에, 입력된 그림 암호의 위치와 등록된 그림 암호의 기준 위치와의 정합 정도가 기준위치에 대한 인증 마진 이내인지 아닌지에 따라 사용자 인증 여부를 결정한다. 여기서, 등록된 그림 암호의 기준 위치는 점(point)이 아니라 소정 영역(predetermined area)일 수도 있다. 또한 제어부(20)는, 둘 이상의 그림 암호의 입력에 의하여 사용자를 인증하는 경우에, 그림 암호 입력 순서의 정합 정도에 따라 사용자 인증 여부를 결정하도록 할 수도 있다.

<76> 저장부(30)는 등록된 그림 암호를 저장하고 있고, 도 1에 도시된 S104 단계를 수행하기 위하여, 사용자가 인증되지 않은 경우에 그림 암호 입력 히스토리를 저장한다.

<77> S106 단계를 수행하기 위하여, 그림 암호 입력 히스토리 분석부(50)는 저장부(30)에 저장된 그림 암호 입력 히스토리를 이용하여 침입 여부를 결정한다. 침입이라고 결정된 경우에 제어부(20)는 S108 단계를 수행하기 위하여, 기준위치에 대한 입력 위치의 인증 마진을 감소시킨다. 그림 암호 입력 히스토리 분석부(50)는, 그림 암호가 등록된 기준 위치로부터 소정 차단 거리 밖에 입력된 경우에는 침입이라고 결정하도록 구현될 수 있다. 또한 제어부(20)는, 인증 마진이 감소된 후에, 그림 암호의 입력 히스토리로부터 침입 결정을 해제할 수 있다고 판단되는 경우에, 감소된 인증 마진을 회복시키는 수단을 더 포함할 수도 있다.

<78> 표시부(60)는 단말기 화면상에 배경 그림을 표시한다. 표시부(60)에 표시된 배경 그림은, 사용자가 그림 암호를 입력하는 위치를 용이하게 찾을 수 있도록 안내하는데 이용될 수 있다.

<79> 도 2 내지 도 4에 도시된 사용자 인증 방법을 수행하는 본 발명에 의한 사용자 인증 장치는, 단말기 화면상에서 그래픽 사용자 인터페이스를 통해 입력된 그림 암호 및 생체 인식 정보에 의해 사용자를 인증하기 위하여, 도 5의 구성요소 중에서 그림 암호 입력부(10), 제어부(20), 저장부(30), 생체 인식부(40), 그림 암호 입력 히스토리 분석부(50)를 포함한다.

<80> S200 단계를 수행하기 위하여, 그림 암호 입력부(10)는 그림 암호가 입력되었는가를 판단한다.

<81> S202 단계 또는 S302 단계를 수행하기 위하여, 제어부(20)는 입력된 그림 암호와 등록된 그림 암호의 정합 정도에 따라 생체 인식의 문턱값을 가변하여 설정한다.

<82> 저장부(30)는 등록된 그림 암호 및 등록된 생체 인식 정보를 저장하고 있다.

<83> S204 단계를 수행하기 위하여, 생체 인식부(40)는 외부로부터 입력된 사용자의 생체 인식 정보와 저장부(30)에 등록된 생체 인식 정보를 비교하여 사용자가 인증되었는가를 결정한다.

<84> 한편 제어부(20)는, S302 단계를 수행하기 위하여, 그림 암호가 입력된 경우에 입력된 그림 암호와 등록된 그림 암호의 정합 정도에 따라 사용자 인증 여부를 결정하도록 구현될 수 있다.

<85> 또한 제어부(20)는, S304 또는 S402 단계를 수행하기 위하여 입력된 그림 암호와 등록된 그림 암호의 정합 정도에 따라 생체 인식의 문턱값을 가변하여 설정하도록 구현될 수 있다.

<86> S302 단계 내지 S312 단계를 수행하기 위하여 제어부(20)는, 입력된 그림 암호의 위치와 저장부(30)에 등록된 기준 위치와의 정합 정도가 인증 마진 이내인지 아닌지에 따라 사용자 인증 여부를 결정하고, 그림 암호에 의하여 사용자가 인증되지 않은 경우에 저장부(30)에 저장된 그림 암호 입력 히스토리를 이용하여 침입 여부를 결정하고, 침입이라고 결정된 경우 기준 위치에 대한 그림 암호 인증 마진을 감소시키도록 구현될 수 있다. 또한 제어부(20)는, 인증 마진이 감소된 후에, 그림 암호의 입력 히스토리로부터 침입 결정을 해제할 수 있다고 판단되는 경우에, 감소된 인증 마진을 회복시키는 수단을 포함할 수도 있다.

<87> 여기서, 등록된 그림 암호의 기준 위치는, 점(point) 개념이 아닌 경계선을 갖는 소정 영역(predetermined area)일 수도 있다. 또한, 제어부(20)는, 둘 이상의 그림 암호

에 의해 사용자를 인증하는 경우에, 그림 암호 입력 순서의 정합 정도에 따라 사용자 인증 여부를 결정하도록 구현될 수도 있다.

<88> S404 단계 및 S412 단계를 수행하기 위하여, 저장부(30)는 그림 암호 입력 히스토리를 저장하고, 제어부(20)는, 생체 인식에 의해 사용자가 인증되지 않은 경우에 그림 암호 입력 히스토리를 이용하여 침입여부를 결정하도록 구현될 수 있다.

<89> S310 단계 또는 S412 단계를 수행함에 있어서 제어부(20)는, 그림 암호가 등록된 기준 위치로부터 소정 차단 거리 밖에 입력된 경우에는 침입이라고 결정하도록 구현될 수도 있다.

<90> S414 단계를 수행하기 위하여 저장부(30)는, 침입이라고 결정된 경우, 침입자의 생체 인식 정보를 저장한다. 이 때 생체 인식부(40)는, 생체 인식 정보 입력값과 저장된 침입자의 생체 인식 정보를 비교하여 인증 여부를 결정하도록 구현될 수 있다.

<91> S416 단계를 수행하기 위하여 제어부(20)는, 사용자가 인증되지 않은 경우에, 그림 암호 입력 히스토리를 이용하여 문턱값의 가변 범위를 재설정하도록 구현될 수 있다. 이 때 제어부(20)는, 잘못된 그림 암호의 입력이 n회 이상인 경우에 보안 수준을 높이도록 문턱값의 가변 범위를 재설정하도록 구현될 수도 있다. 또한, 제어부(20)는, 보안 수준을 높이도록 문턱값의 가변 범위를 재설정한 후에, 올바른 그림 암호의 입력이 m회 이상인 경우, 문턱값의 가변 범위를 환원하도록 구현될 수도 있다.

<92> 표시부(60)는 단말기 화면상에 배경 그림을 표시한다. 표시부(60)에 표시된 배경 그림은, 사용자가 그림 암호를 입력하는 위치를 용이하게 찾을 수 있도록 안내하는데 이용될 수 있다.

<93> 본 발명에 의한 사용자 인증 장치는, 도 4에 도시된 S408 단계 및 S410 단계를 수행하기 위하여, 생체 인식부에 의해 사용자가 인증된 경우에, 인증키를 추가/갱신하도록 구현될 수 있다. 인증키를 추가/갱신하기 위하여, 생체 인식부(40)는 인증이 성공한 경우에, 획득된 생체 인식 정보를 저장부(30)로 출력한다. 특히, 생체 인식부(40)는, 인증키 갱신의 신뢰성을 높이기 위하여, 그림 암호 입력부(10) 입력된 그림 암호가 등록된 그림 암호와 일치하고, 생체 인식부(40)에 의해 사용자가 인증된 경우에만, 획득된 생체 인식 정보를 저장부(30)로 출력하여, 인증키를 추가/갱신하도록 구현될 수 있다. 또한 본 발명에 의한 사용자 인증 장치는, 입력된 생체 인식 정보와 등록된 생체 인식 정보의 정합 정도가 소정 문턱값 이상인 경우에만 인증키를 추가/갱신하도록 구현될 수도 있다.

<94> 한편, 전술한 본 발명의 바람직한 실시예에 의한 그림 암호에 의한 사용자 인증 방법 및 그림 암호와 생체 인식을 결합한 형태의 사용자 인증 방법(도 1 내지 도 4)은 컴퓨터에서 실행될 수 있는 프로그램으로 작성가능하고, 컴퓨터로 읽을 수 있는 기록매체를 이용하여 상기 프로그램을 동작시키는 범용 디지털 컴퓨터에서 구현될 수 있다. 상기 컴퓨터로 읽을 수 있는 기록매체는 예컨데 롬, 플로피 디스크, 하드디스크 등과 같은 마그네틱 저장매체, 예컨데 씨디롬, 디브이디 등과 같은 광학적 판독매체, 및 예컨데 인터넷을 통한 전송과 같은 캐리어 웨이브와 같은 저장매체를 포함한다.

【발명의 효과】

<95> 이상에서 설명한 바와 같이, 본 발명에 의한 사용자 인증 방법 및 장치에 의하면, 키 조작부가 없는 PDA 등에서의 그림 암호에 의한 사용자 인증에 있어서, 편의성, 신뢰성 및 보안성을 확보할 수 있다.

<96> 또한 그림 암호에 의한 사용자 인증 결과에 따라 생체 인식을 위한 문턱값을 가변함으로써, 생체 인식기의 불완전한 인증 성능을 개선하여, FAR과 FRR을 동시에 낮출 수 있는 사용자 인증이 이루어지는 효과가 있다.

<97> 본 발명은 이상에서 설명되고 도면들에 표현된 예시들에 한정되는 것은 아니다. 전술한 실시 예들에 의해 가르침 받은 당업자라면, 다음의 특허 청구 범위에 기재된 본 발명의 범위 및 목적 내에서 치환, 소거, 병합, 및 단계들의 재배치 등에 의하여 전술한 실시 예들에 대해 많은 변형이 가능할 것이다.

【특허청구범위】

【청구항 1】

단말기 화면상에서 그래픽 사용자 인터페이스를 통해 입력된 그림 암호에 의해 사용자를 인증하는 방법에 있어서,

상기 그림 암호가 입력되었는가를 판단하는 단계;

상기 그림 암호가 입력된 경우에, 상기 입력된 그림 암호의 위치와 등록된 그림 암호의 기준 위치와의 정합 정도가 기준위치에 대한 인증 마진 이내인지 아닌지에 따라 사용자 인증 여부를 결정하는 단계;

인증되지 않은 경우에는 그림 암호 입력 히스토리를 저장하는 단계;

상기 그림 암호 입력 히스토리를 이용하여 침입 여부를 결정하는 단계; 및

침입이라고 결정된 경우, 상기 기준위치에 대한 입력 위치의 인증 마진을 감소시키는 단계를 포함하는 것을 특징으로 하는 그림 암호에 의한 사용자 인증 방법.

【청구항 2】

제1항에 있어서,

상기 등록된 기준 위치는 소정 영역인 것을 특징으로 하는 그림 암호에 의한 사용자 인증 방법.

【청구항 3】

제1항 또는 제2항에 있어서,

상기 사용자 인증 여부를 결정하는 단계는, 상기 그림 암호 입력 순서의 정합 정도에 따라 사용자 인증 여부를 결정하는 단계를 더 포함하는 것을 특징으로 하는 그림 암호에 의한 사용자 인증 방법.

【청구항 4】

제1항에 있어서, 상기 침입 여부를 결정하는 단계에 있어서,

상기 그림 암호가 상기 등록된 기준 위치로부터 소정 차단 거리 밖에 입력된 경우에는 침입이라고 결정하는 것을 특징으로 하는 그림 암호에 의한 사용자 인증 방법.

【청구항 5】

제1항에 있어서,

상기 단말기 화면상에 배경 그림을 표시하는 단계를 더 포함하는 것을 특징으로 하는 그림 암호에 의한 사용자 인증 방법.

【청구항 6】

제1항에 있어서,

침입이라고 결정되어 인증 마진이 감소된 후에, 그림 암호의 입력 히스토리로부터 침입 결정을 해제할 수 있다고 판단되는 경우에는, 감소된 인증 마진을 회복시키는 단계를 더 포함하는 것을 특징으로 하는 그림 암호에 의한 사용자 인증 방법.

【청구항 7】

단말기 화면상에서 그래픽 사용자 인터페이스를 통해 입력된 그림 암호와, 생체 인식 정보에 의하여 사용자를 인증하는 방법에 있어서,

(a) 상기 그림 암호가 입력되었는가를 판단하는 단계;

(b) 상기 그림 암호가 입력된 경우에, 상기 입력된 그림 암호와 등록된 그림 암호의 정합 정도에 따라 생체 인식의 문턱값을 가변하여 설정하는 단계;

(c) 외부로부터 입력된 사용자의 생체 인식 정보와 등록된 생체 인식 정보를 비교하여 사용자가 인증되었는가를 판단하고, 사용자가 인증되지 않은 경우에는 상기 (a) 단계로 진행하는 단계를 포함하는 것을 특징으로 하는 사용자 인증 방법.

【청구항 8】

제7항에 있어서, 상기 (b) 단계는,

(b1) 상기 그림 암호가 입력된 경우에, 상기 입력된 그림 암호와 등록된 그림 암호의 정합 정도에 따라 사용자 인증 여부를 결정하는 단계; 및

(b2) 상기 그림 암호에 의해 사용자 인증이 허가된 경우에, 상기 입력된 그림 암호와 등록된 그림 암호의 정합 정도에 따라 생체 인식의 문턱값을 가변하여 설정하는 단계를 포함하는 것을 특징으로 하는 사용자 인증 방법.

【청구항 9】

제8항에 있어서, 상기 (b1) 단계는,

(b10) 상기 그림 암호가 입력된 경우에, 상기 입력된 그림 암호의 위치와 등록된 기준 위치와의 정합 정도가 인증 마진 이내인지 아닌지에 따라 사용자 인증 여부를 결정하는 단계; 및

(b12) 상기 그림 암호 입력에 의하여 인증되지 않은 경우에, 그림 암호 입력 히스토리를 저장하는 단계;

(b14) 상기 그림 암호 입력 히스토리를 이용하여 침입 여부를 결정하는 단계; 및

(b16) 침입이라고 결정된 경우, 상기 기준 위치에 대한 상기 그림 암호 인증 마진을 감소시키는 단계를 포함하는 것을 특징으로 하는 사용자 인증 방법.

【청구항 10】

제9항에 있어서, 상기 등록된 기준 위치는,

소정 영역인 것을 특징으로 하는 사용자 인증 방법.

【청구항 11】

제9항 또는 제10항에 있어서, 상기 (b10) 단계는,

그림 암호 입력 순서의 정합 정도에 따라 사용자 인증 여부를 결정하는 단계를 더 포함하는 것을 특징으로 하는 사용자 인증 방법.

【청구항 12】

제9항에 있어서, 상기 (b14) 단계는,

상기 그림 암호가 상기 등록된 기준 위치로부터 소정 차단 거리 밖에 입력된 경우에는 침입이라고 결정하는 것을 특징으로 하는 사용자 인증 방법.

【청구항 13】

제7항에 있어서,

(b18) 침입이라고 결정되어 인증 마진이 감소된 후에, 그림 암호의 입력 히스토리로부터 침입 결정을 해제할 수 있다고 판단되는 경우에는, 감소된 인증 마진을 회복시키는 단계를 더 포함하는 것을 특징으로 하는 사용자 인증 방법.

【청구항 14】

제7항에 있어서,

상기 단말기 화면상에 배경 그림을 표시하는 단계를 더 포함하는 것을 특징으로 하는 사용자 인증 방법.

【청구항 15】

제7항에 있어서,

(d) 상기 (b) 단계 후에, 그림 암호 입력 히스토리를 저장하는 단계; 및

(e) 상기 (c) 단계 후에, 사용자가 인증되지 않은 경우에는 상기 그림 암호 입력 히스토리를 이용하여 침입여부를 결정하여, 침입이 아니라고 결정되면 상기 (a) 단계로 진행하는 단계;를 포함하는 것을 특징으로 하는 사용자 인증 방법.

【청구항 16】

제15항에 있어서,

(f) 상기 (e) 단계의 판단 결과 침입이라고 결정된 경우, 입력된 침입자의 생체 인식 정보를 저장하는 단계를 더 포함하고,

상기 (c) 단계는 생체 인식기 입력값과 상기 저장된 침입자의 생체 인식 정보를 비교하여 인증하는 단계를 포함하는 것을 특징으로 하는 사용자 인증 방법.

【청구항 17】

제7항에 있어서,

(d) 상기 (b) 단계 후에, 그림 암호 입력 히스토리를 저장하는 단계; 및

(g) 상기 (c) 단계 후에, 사용자가 인증되지 않은 경우에는 상기 그림 암호 입력 히스토리를 이용하여 상기 문턱값의 가변 범위를 변경하고 상기 (a) 단계로 진행하는 단계를 포함하는 것을 특징으로 하는 사용자 인증 방법.

【청구항 18】

제17항에 있어서, 상기 (g) 단계는,

잘못된 그림 암호의 입력이 n회 이상인 경우에 보안 수준을 높이도록 상기 문턱값의 가변 범위를 변경하는 것을 특징으로 하는 사용자 인증 방법.

【청구항 19】

제18항에 있어서, 상기 (g) 단계는,

보안 수준을 높이도록 상기 문턱값의 가변 범위를 변경한 후에, 올바른 그림 암호의 입력이 m회 이상인 경우, 상기 문턱값의 가변 범위를 환원하는 단계를 포함하는 것을 특징으로 하는 사용자 인증 방법.

【청구항 20】

제7항에 있어서,

(h) 상기 (c) 단계에서 상기 생체 인식기에 의해 사용자가 인증된 경우에, 인증키를 추가/갱신하는 단계를 포함하는 것을 특징으로 하는 사용자 인증 방법.

【청구항 21】

제20항에 있어서, 상기 (h) 단계는,

상기 입력된 그림 암호가 등록된 그림 암호와 일치하고, 상기 생체 인식기에 의해 사용자가 인증된 경우에만 인증키를 추가/갱신하는 것을 특징으로 하는 사용자 인증 방법.

【청구항 22】

제20항 또는 제21항에 있어서, 상기 (h) 단계는,

상기 생체 인식기에 의해 사용자가 인증된 경우, 입력된 생체 인식 정보와 등록된 생체 인식 정보의 정합 정도가 소정 문턱값 이상인 경우에만 인증키를 추가/갱신하는 것을 특징으로 하는 사용자 인증 방법.

【청구항 23】

단말기 화면상에서 그래픽 사용자 인터페이스를 통해 입력된 그림 암호에 의해 사용자를 인증하는 장치에 있어서,

상기 그림 암호가 입력되었는가를 판단하는 그림 암호 입력부;

상기 그림 암호가 입력된 경우에, 상기 입력된 그림 암호의 위치와 등록된 그림 암호의 기준 위치와의 정합 정도가 기준위치에 대한 인증 마진 이내인지 아닌지에 따라 사용자 인증 여부를 결정하는 제어부;

상기 등록된 그림 암호를 저장하고 있고, 인증되지 않은 경우에는 그림 암호 입력 히스토리를 저장하는 저장부;

상기 그림 암호 입력 히스토리를 이용하여 침입 여부를 결정하는 그림 암호 입력 히스토리 분석부를 포함하고,

침입이라고 결정된 경우에 상기 제어부는, 상기 기준위치에 대한 입력 위치의 인증 마진을 감소시키는 것을 특징으로 하는 그림 암호에 의한 사용자 인증 장치.

【청구항 24】

제23항에 있어서,

상기 등록된 기준 위치는 소정 영역인 것을 특징으로 하는 그림 암호에 의한 사용자 인증 장치.

【청구항 25】

제23항 또는 제24항에 있어서, 상기 제어부는,

상기 그림 암호 입력 순서의 정합 정도에 따라 사용자 인증 여부를 결정하는 것을 특징으로 하는 그림 암호에 의한 사용자 인증 장치.

【청구항 26】

제23항에 있어서, 상기 그림 암호 입력 히스토리 분석부는,

상기 그림 암호가 상기 등록된 기준 위치로부터 소정 차단 거리 밖에 입력된 경우에는 침입이라고 결정하는 것을 특징으로 하는 그림 암호에 의한 사용자 인증 장치.

【청구항 27】

제23항에 있어서,

상기 단말기 화면상에 배경 그림을 표시하는 표시부를 더 포함하는 그림 암호에 의한 사용자 인증 장치.

【청구항 28】

제23항에 있어서, 상기 제어부는,

인증 마진이 감소된 후에, 그림 암호의 입력 히스토리로부터 침입 결정을 해제할 수 있다고 판단되는 경우에, 감소된 인증 마진을 회복시키는 수단을 더 포함하는 것을 특징으로 하는 그림 암호에 의한 사용자 인증 장치.

【청구항 29】

단말기 화면상에서 그래픽 사용자 인터페이스를 통해 입력된 그림 암호와, 생체 인식 정보에 의하여 사용자를 인증하는 장치에 있어서,

상기 그림 암호가 입력되었는가를 판단하는 그림 암호 입력부;

등록된 그림 암호 및 등록된 생체 인식 정보를 저장하고 있는 저장부;

상기 그림 암호가 입력된 경우에, 상기 입력된 그림 암호와 등록된 그림 암호의 정합 정도에 따라 생체 인식의 문턱값을 가변하여 설정하는 제어부;

외부로부터 입력된 사용자의 생체 인식 정보와 등록된 생체 인식 정보를 비교하여 사용자가 인증되었는가를 결정하는 생체 인식부를 포함하는 것을 특징으로 하는 사용자 인증 장치.

【청구항 30】

제29항에 있어서, 상기 제어부는,

상기 그림 암호가 입력된 경우에 상기 입력된 그림 암호와 등록된 그림 암호의 정합 정도에 따라 사용자 인증 여부를 결정하고,

상기 입력된 그림 암호와 등록된 그림 암호의 정합 정도에 따라 생체 인식의 문턱값을 가변하여 설정하는 것을 특징으로 하는 사용자 인증 장치.

【청구항 31】

제30항에 있어서,

상기 제어부는, 상기 그림 암호가 입력된 경우에, 상기 입력된 그림 암호의 위치와 등록된 기준 위치와의 정합 정도가 인증 마진 이내인지 아닌지에 따라 사용자 인증 여부를 결정하고, 사용자가 인증되지 않은 경우에 상기 그림 암호 입력 히스토리를 이용하여 침입 여부를 결정하고, 침입이라고 결정된 경우 상기 기준 위치에 대한 상기 그림 암호 인증 마진을 감소시키고,

상기 저장부는, 상기 그림 암호 입력에 의하여 인증되지 않은 경우에 그림 암호 입력 히스토리를 저장하는 것을 특징으로 하는 사용자 인증 장치.

【청구항 32】

제31항에 있어서, 상기 등록된 기준 위치는,

소정 영역인 것을 특징으로 하는 사용자 인증 장치.

【청구항 33】

제31항 또는 제32항에 있어서, 상기 제어부는,

그림 암호 입력 순서의 정합 정도에 따라 사용자 인증 여부를 결정하는 수단을 포함하는 것을 특징으로 하는 사용자 인증 장치.

【청구항 34】

제31항에 있어서, 상기 제어부는,

상기 그림 암호가 상기 등록된 기준 위치로부터 소정 차단 거리 밖에 입력된 경우에는 침입이라고 결정하는 것을 특징으로 하는 사용자 인증 장치.

【청구항 35】

제31항에 있어서, 상기 제어부는,

인증 마진이 감소된 후에, 그림 암호의 입력 히스토리로부터 침입 결정을 해제할 수 있다고 판단되는 경우에, 감소된 인증 마진을 회복시키는 수단을 포함하는 것을 특징으로 하는 사용자 인증 장치.

【청구항 36】

제29항에 있어서,

상기 단말기 화면상에 배경 그림을 표시하는 표시부를 더 포함하는 것을 특징으로 하는 사용자 인증 장치.

【청구항 37】

제29항에 있어서,

상기 저장부는, 그림 암호 입력 히스토리를 저장하고,

상기 제어부는, 사용자가 인증되지 않은 경우에 상기 그림 암호 입력 히스토리를 이용하여 침입여부를 결정하는 것을 특징으로 하는 사용자 인증 장치.

【청구항 38】

제37항에 있어서,

상기 저장부는, 침입이라고 결정된 경우, 입력된 침입자의 생체 인식 정보를 저장하고,

상기 생체 인식부는, 생체 인식 정보 입력값과 상기 저장된 침입자의 생체 인식 정보를 비교하여 인증 여부를 결정하는 것을 특징으로 하는 사용자 인증 장치.

【청구항 39】

제29항에 있어서,

상기 저장부는, 그림 암호 입력 히스토리를 저장하고,

상기 제어부는, 사용자가 인증되지 않은 경우에, 상기 그림 암호 입력 히스토리를 이용하여 상기 문턱값의 가변 범위를 재설정하는 것을 특징으로 하는 사용자 인증 장치.

【청구항 40】

제39항에 있어서, 상기 제어부는,

잘못된 그림 암호의 입력이 n회 이상인 경우에 보안 수준을 높이도록 상기 문턱값의 가변 범위를 재설정하는 것을 특징으로 하는 사용자 인증 장치.

【청구항 41】

제40항에 있어서, 상기 제어부는,

보안 수준을 높이도록 상기 문턱값의 가변 범위를 재설정한 후에, 올바른 그림 암호의 입력이 m회 이상인 경우, 상기 문턱값의 가변 범위를 환원하는 것을 특징으로 하는 사용자 인증 장치.

【청구항 42】

제29항에 있어서,

상기 생체 인식부에 의해 사용자가 인증된 경우에, 생체 인증키를 추가/갱신하는 수단을 포함하는 것을 특징으로 하는 사용자 인증 장치.

【청구항 43】

제42항에 있어서,

상기 입력된 그림 암호가 상기 등록된 그림 암호와 일치하고, 상기 생체 인식부에 의해 사용자가 인증된 경우에만 인증키를 추가/갱신하는 것을 특징으로 하는 사용자 인증 장치.

【청구항 44】

제42항 또는 제43항에 있어서,

상기 생체 인식기에 의해 사용자가 인증된 경우, 입력된 생체 인식 정보와 등록된 생체 인식 정보의 정합 정도가 소정 문턱값 이상인 경우에만 인증키를 추가/갱신하는 것을 특징으로 하는 사용자 인증 장치.

【청구항 45】

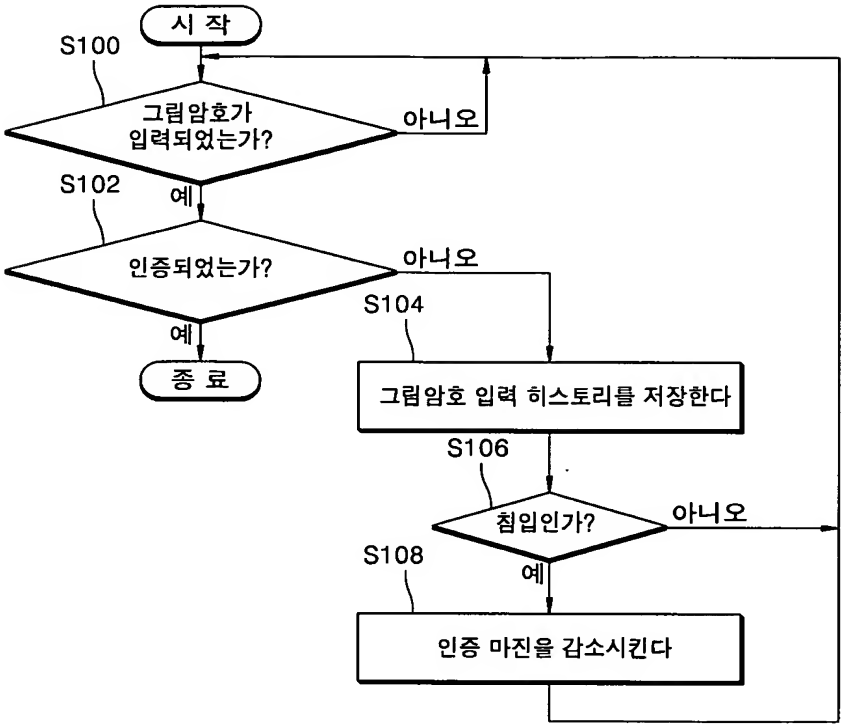
제1항 내지 제6항에 기재된 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

【청구항 46】

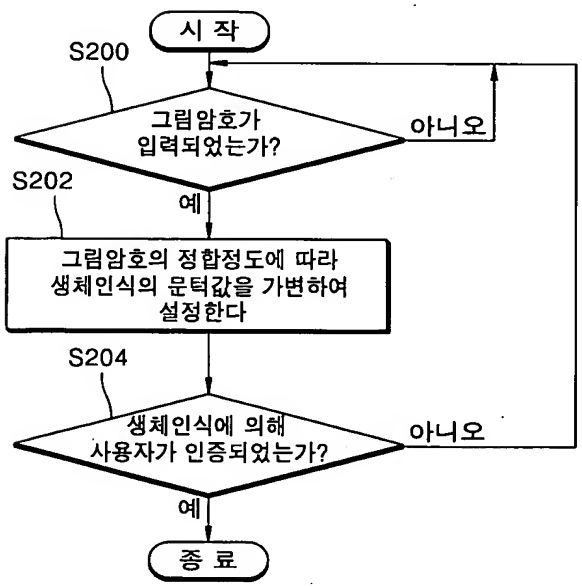
제7항 내지 제22항에 기재된 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

【도면】

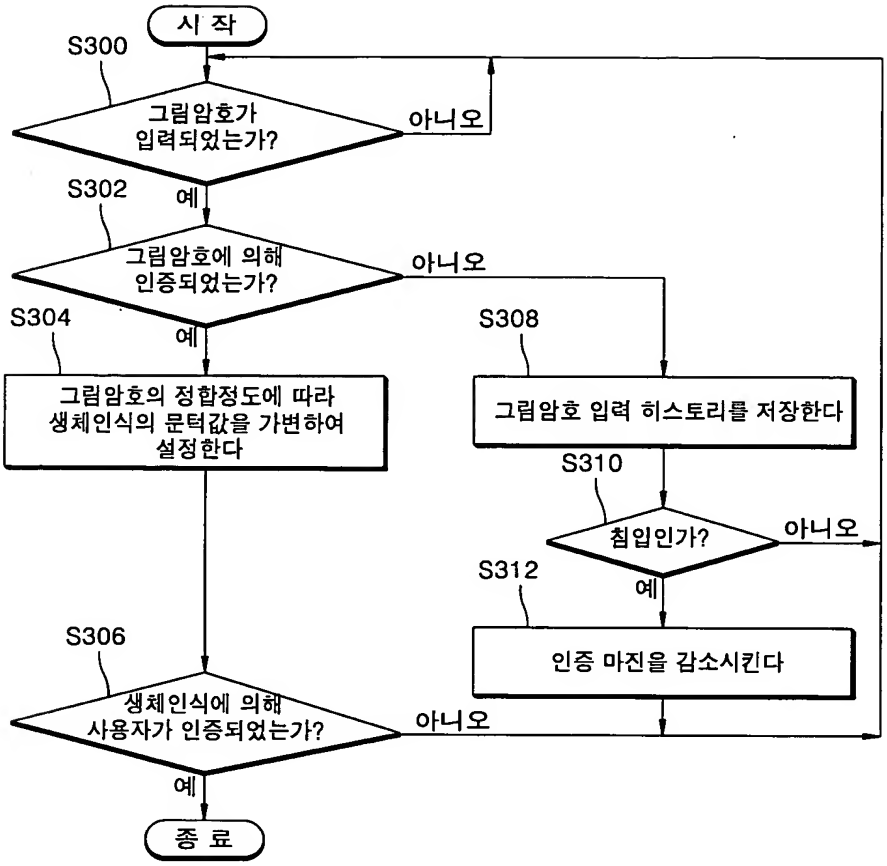
【도 1】


시 작
S100
그림암호가 입력되었는가?
아니오
예
S102
인증되었는가?
아니오
예
종 료
S104
그림암호 입력 히스토리를 저장한다
S106
침입인가?
아니오
예
S108
인증 마진을 감소시킨다

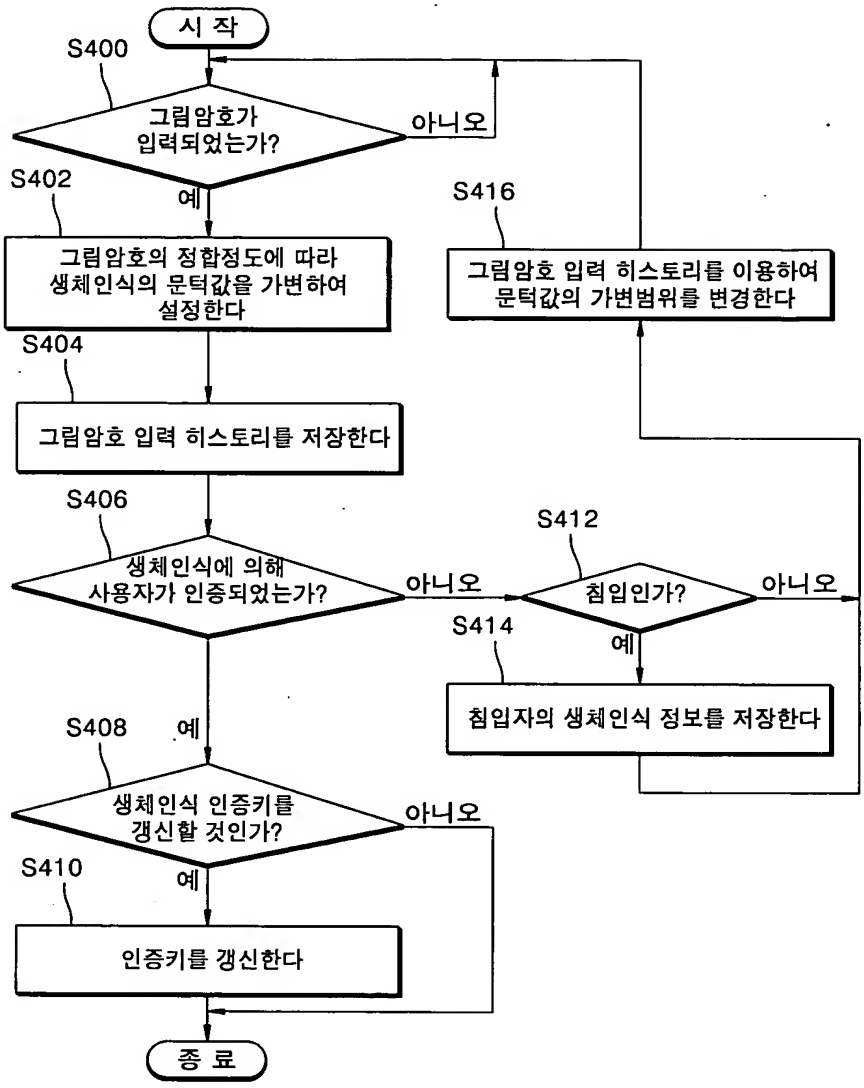
【도 2】


시 작
S200
그림암호가 입력되었는가?
아니오
예
S202
그림암호의 정합정도에 따라 생체인식의 문턱값을 가변하여 설정한다
S204
생체인식에 의해 사용자가 인증되었는가?
아니오
예
종 료

【도 3】


시 작
S300
그림암호가 입력되었는가?
아니오
예
S302
그림암호에 의해 인증되었는가?
아니오
예
S304
그림암호의 정합정도에 따라 생체인식의 문턱값을 가변하여 설정한다
S308
그림암호 입력 히스토리를 저장한다
S310
침입인가?
아니오
예
S312
인증 마진을 감소시킨다
S306
생체인식에 의해 사용자가 인증되었는가?
아니오
예
종 료

【도 4】


시 작
S400
그림암호가 입력되었는가?
아니오
예
S402
그림암호의 정합정도에 따라 생체인식의 문턱값을 가변하여 설정한다
S404
그림암호 입력 히스토리를 저장한다
S406
생체인식에 의해 사용자가 인증되었는가?
아니오
예
S408
생체인식 인증키를 갱신할 것인가?
아니오
예
S410
인증키를 갱신한다
종 료
S412
침입인가?
아니오
예
S414
침입자의 생체인식 정보를 저장한다
S416
그림암호 입력 히스토리를 이용하여 문턱값의 가변범위를 변경한다

【도 5】